Windows Server 2008 Quick Reference Guide

Windows Server 2008 is the latest and greatest Windows Server Platform available from Microsoft. With its enhancements in Active Directory, DNS Management, and infrastructure coordination, Server 2008 has set the bar to the highest level that Microsoft has ever attempted. Accordingly, with the new features of Windows Server 2008, new challenges have arisen in how these technologies should be administered. Therefore, LearnSmart has released this quick reference guide for you, free to download, as a useful tool in your process of administering your network.

The Quick Reference Guide helps experienced and new Windows Server Administrators navigate Server 2008's new features more quickly and effectively. For those of you who've worked with previous versions of Windows Server, the Windows Server 2008 Quick Reference Guide helps you pinpoint and master the new and expanded capabilities of the 2008 edition. Use this Quick Reference Guide to bring your fresh, new Server 2008 expertise to the table and get ahead of the curve at your company. For those of you just getting started, the Windows Server 2008 Quick Reference Guide will help you become more competitive with the other members in your field. For more information and training for Server 2008, or any other IT skills and certifications, you can always contact LearnSmart at 1-800-418-6789. Enjoy your Windows Server 2008 Quick Reference Guide.

Windows Server 2008 Improvements

Active Directory Lightweight Directory Services

A replacement for Active Directory Application Mode, Active Directory Lightweight Directory Services (AD LDS) is a system used in Windows Server 2008 to provide directory services for applications requiring access to specific directories. It is domain and forest independent, and provides an extra level of security so applications do not have direct access to the system files. The figure on the next page outlines the features of AD LDS.

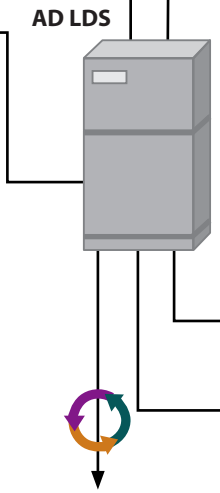
Active Directory Lightweight Directory Services

AD LDS Usage Scenarios

- Application-Specific Directory Services Scenarios
- Application Development Scenarios
- Extranet Access Management
- X.500/LDAP Directory Migration Scenarios
- Deployment in Datacenters and Perimeter Networks (Branch Offices, DMZs)

AD LDS Users and Groups

- AD LDS authenticates the identity of users who are represented by AD LDS user objects
- AD LDS allows the use of Windows Security principles from the local machine and AD for access control. Authentication process for these user principles is redirected to the local machine and AD respectively
- Four default groups: Administrators, Instances, Readers, and Users



AD LDS Tools

- ADScema Analyzer
  Helps migrate the AD schema to AD LDS, from one AD LDS instance to another, or from any LDAP- compliant directory to an AD LDS instance
- Active Directory to AD LDS Synchronizer
  Command-line tool that synchronizes data from an AD forest to a configuration set of an AD LDS database
- Snapshot Browser
  Uses LDAP client to bind to VSS snapshot (taken by NTDS UTIL) and view read-only instance of AD LDS database
- Active Directory Sites and Services
  Assists in administrating AD LDS replication topology
- Install from Media (IFM)
  IFM can also be used to install an AD LDS

AD LDS Platform Support

- AD LDS is a Windows Server 2008 role

AD LDS Access Control

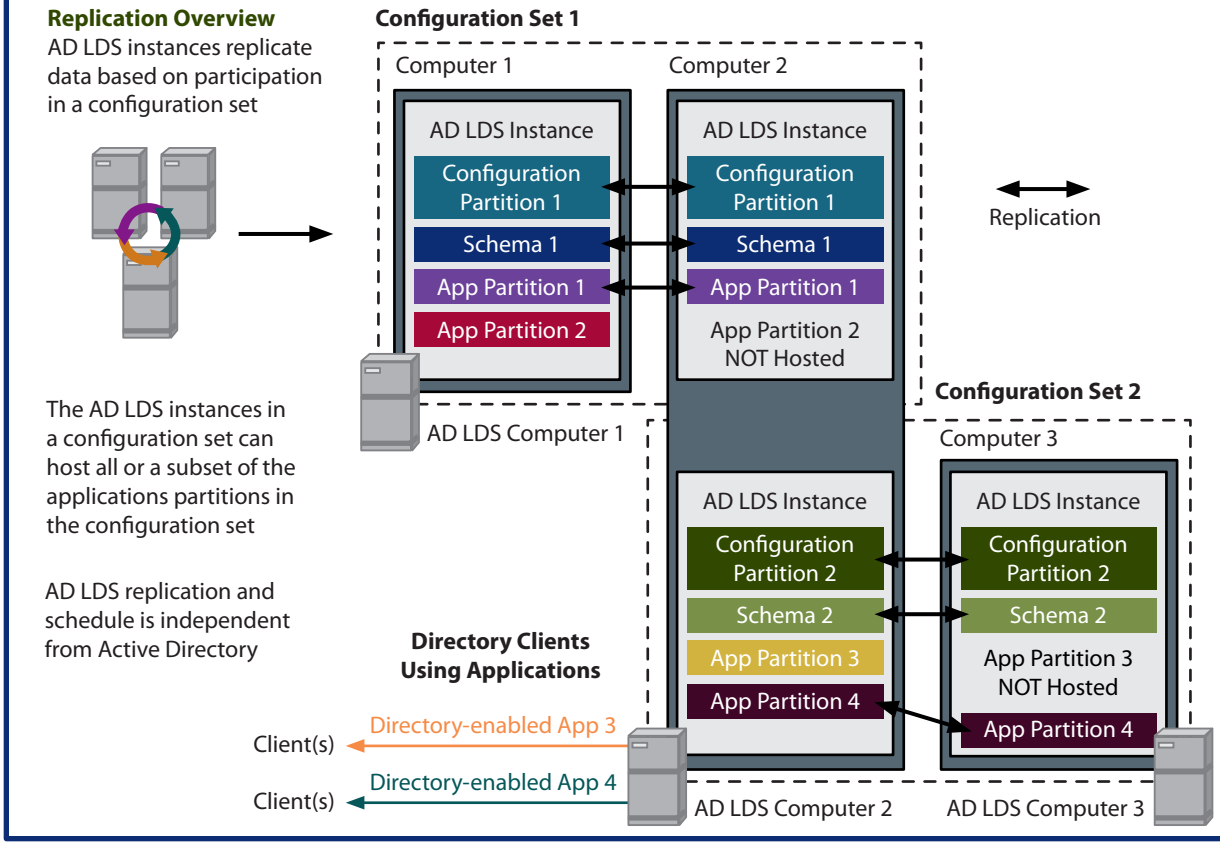
- Uses ACLs on directory objects to determine which objects user can access

Replication Overview

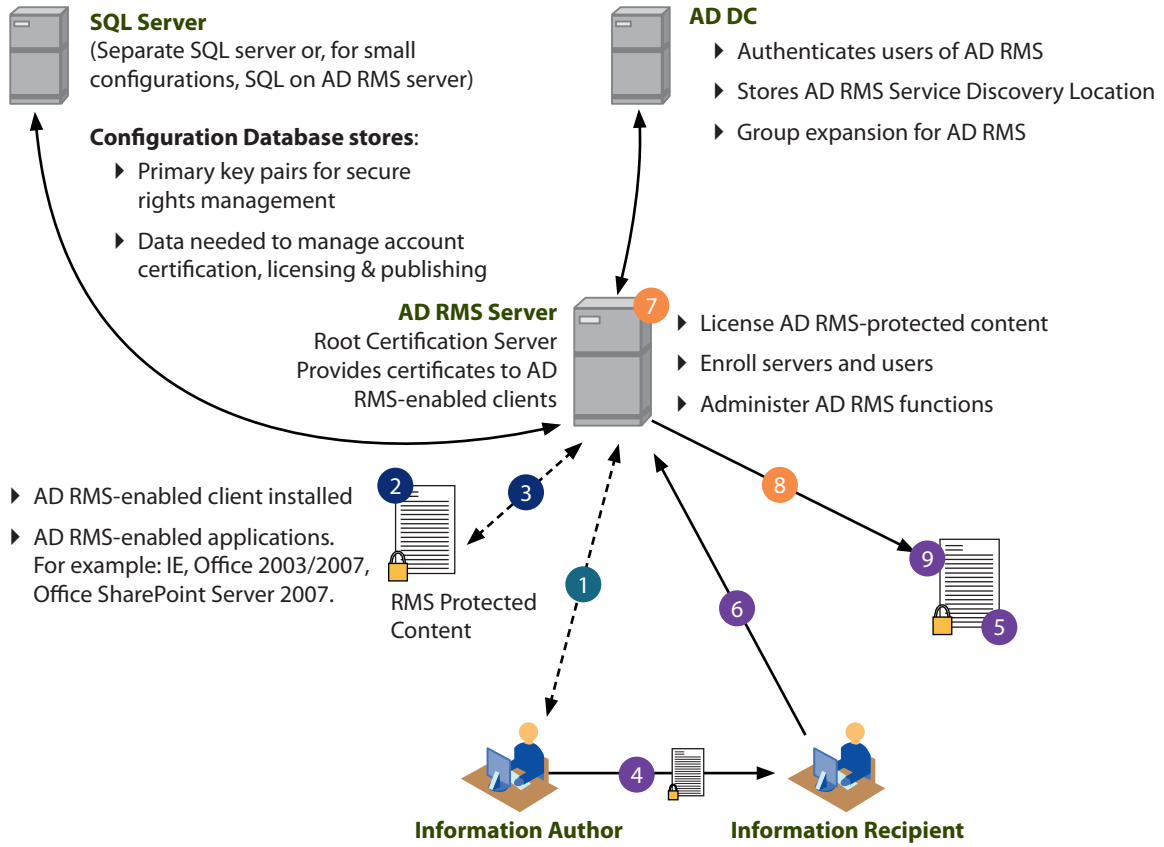
AD LDS instances replicate data based on participation in a configuration set

The AD LDS instances in a configuration set can host all or a subset of the applications partitions in the configuration set

AD LDS replication and schedule is independent from Active Directory

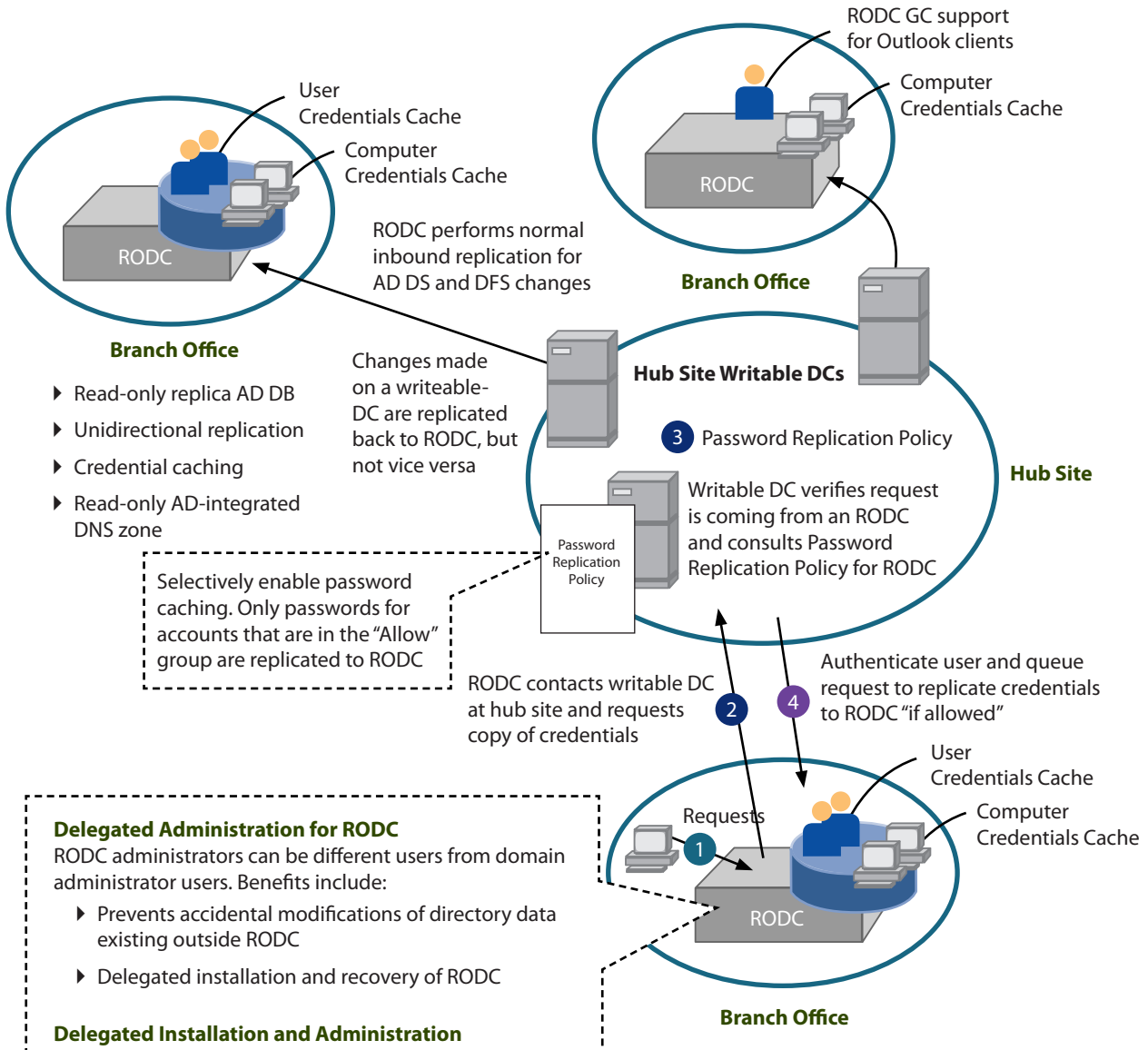


Active Directory Rights Management Services


SQL Server
(Separate SQL server or, for small configurations, SQL on AD RMS server)
Configuration Database stores:
Primary key pairs for secure rights management
Data needed to manage account certification, licensing & publishing
AD DC
Authenticates users of AD RMS
Stores AD RMS Service Discovery Location
Group expansion for AD RMS
AD RMS Server
Root Certification Server
Provides certificates to AD RMS-enabled clients
License AD RMS-protected content
Enroll servers and users
Administer AD RMS functions
AD RMS-enabled client installed
AD RMS-enabled applications. For example: IE, Office 2003/2007, Office SharePoint Server 2007.
RMS Protected Content
Information Author
Information Recipient

1. Author uses AD RMS for the first time - receives Rights Account Certificate (RAC) and Client Licensor Certificate (CLC). Happens once and enables user to publish online or offline and consume rights-protected content.
2. Using AD RMS-enabled application, author creates file and specifies user rights. Policy license containing user policies is generated.
3. Application generates content key, encrypts content with it. Online Publish - Encrypts content key with AD RMS server public key and sends to AD RMS server. Server creates and signs publishing license (PL). Offline Publish - Encrypts content key with CLC public key, encrypts copy of key with AD RMS server public key. Creates PL and signs with CLC private key. Append PL to encrypted content.
4. AD RMS-protected content file sent to Information Recipient. AD RMS-protected content may also be represented by e-mail.
5. Recipient receives file, opens using AD RMS-enabled application or browser. If no account certificate on the current computer, the AD RMS server will issue one (AD RMS document notifies application of the AD RMS server URL).
6. Application sends request for use license to AD RMS server that issued publishing license (if file published offline, send to server that issued the CLC). Request includes RAC and PL for file.
7. AD RMS server confirms recipient is authorized, checks for a named user, and creates use license for the user. Server decrypts content key using private key of server and re-encrypts content key with public key of recipient, then adds encrypted session key to the use license. This means only the intended recipient can access the file.
8. AD RMS server sends use license to information recipient's computer.
9. Application examines both the license and the recipient's account certificate to determine whether any certificate in either chain of trust requires a revocation list. User granted access as specified by information author.

Active Directory Read-Only Domain Controller


RODC GC support for Outlook clients
Computer Credentials Cache
RODC
Branch Office
User Credentials Cache
Computer Credentials Cache
RODC
RODC performs normal inbound replication for AD DS and DFS changes
Branch Office
Changes made on a writeable-DC are replicated back to RODC, but not vice versa
Hub Site Writable DCs
3 Password Replication Policy
Hub Site
Writable DC verifies request is coming from an RODC and consults Password Replication Policy for RODC
Password Replication Policy
Selectively enable password caching. Only passwords for accounts that are in the "Allow" group are replicated to RODC
RODC contacts writable DC at hub site and requests copy of credentials
2
4
Authenticate user and queue request to replicate credentials to RODC "if allowed"
User Credentials Cache
Computer Credentials Cache
Requests
1
RODC
Branch Office

- Read-only replica AD DB
- Unidirectional replication
- Credential caching
- Read-only AD-integrated DNS zone

Delegated Administration for RODC

RODC administrators can be different users from domain administrator users. Benefits include:

- Prevents accidental modifications of directory data existing outside RODC
- Delegated installation and recovery of RODC

Delegated Installation and Administration Process for RODC

(Note: Steps 1 and 2 are not necessarily performed from the same computer)

1. **Pre-Create and Delegate**
   - Domain Administrator uses AD Users and Computers MMC snap-in to pre-create RODC
   - Specifies RODC's FQDN and Delegated Administration group
2. **Promote RODC**
   - Delegated Administrator (non-DA) uses DCPROMO Wizard from server to configure as RODC
   - Replicates over network, with support for secure IFM
   - Reboots as RODC

New Group Policy Features

Group Policy Delivery and Enforcement

Workstation / Member Server Delivery

- Workstation / Member Server Startup
- Processed every 90-120 minutes (random)
- Refreshes on NLA notifications (Windows Vista and Windows Server 2008)

User Delivery

- At user logon
- Processed approximately every 90-120 minutes (random)

Domain Controller Delivery

- Domain Controller Startup
- Processed approximately every 5 minutes

Network Location Awareness

Using Network Location Awareness, Group Policy has access to resource detection and event notification capabilities in the operating system. This allows Group Policy to refresh after detecting the following events:

- Recovery from hibernation or standby
- Establishment of VPN sessions
- Moving in or out of a wireless network

Network Location Awareness also:

- Removes the reliance on the ICMP protocol (PING) for assisting policy application across slow link connections
- Is used for bandwidth determination (applying GP over slow links)

Group Policy Tools

Windows Vista, Windows Server 2008

- Manage new Windows Vista/Windows Server 2008 Policy Settings
- Manage Windows 2000, Windows Server 2003, and Windows XP Machine Policy Settings

Windows 2000, Windows Server 2003, Windows XP

- *Cannot* manage new Windows Vista/ Windows Server 2008 Policy Settings
- Manage Windows 2000, Windows Server 2003 and Windows XP Machine Policy Settings

Group Policy Central Store

Central Storage for Administrative Templates

1) Create Central Store on PDC Emulator
2) Central Store created for each domain
3) If Central Store available when administering domain-based GPOs, the central store is used by default

- Policies
  - [GUID]
  - ADM
  - Policy Definitions (stores all ".admx" files)
    - en-US (All ".adml" files stored in language-specific folders. For example, "en-US" for US English)

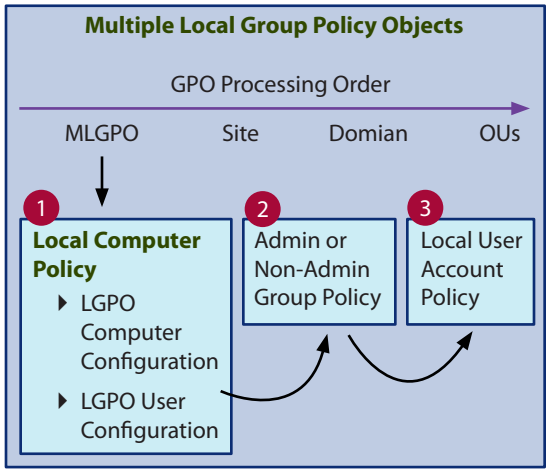
Advantages of Central Store include reduced SYSVOL size and reduced traffic between DCs

FRS/ DFS-R
Use File Replication Service (FRS) on Windows 2000 and Windows Server 2003
Use Distributed File System Replication (DFS-R) on Windows Server 2008
Forest functional environment

Central Store Benefits

- Single point of storage
- Multilingual support
- Central Store hosted on Windows Server 2000, Windows Server 2003, & Windows Server 2008

Multiple Local Group Policy Objects



Active Directory Federation Services

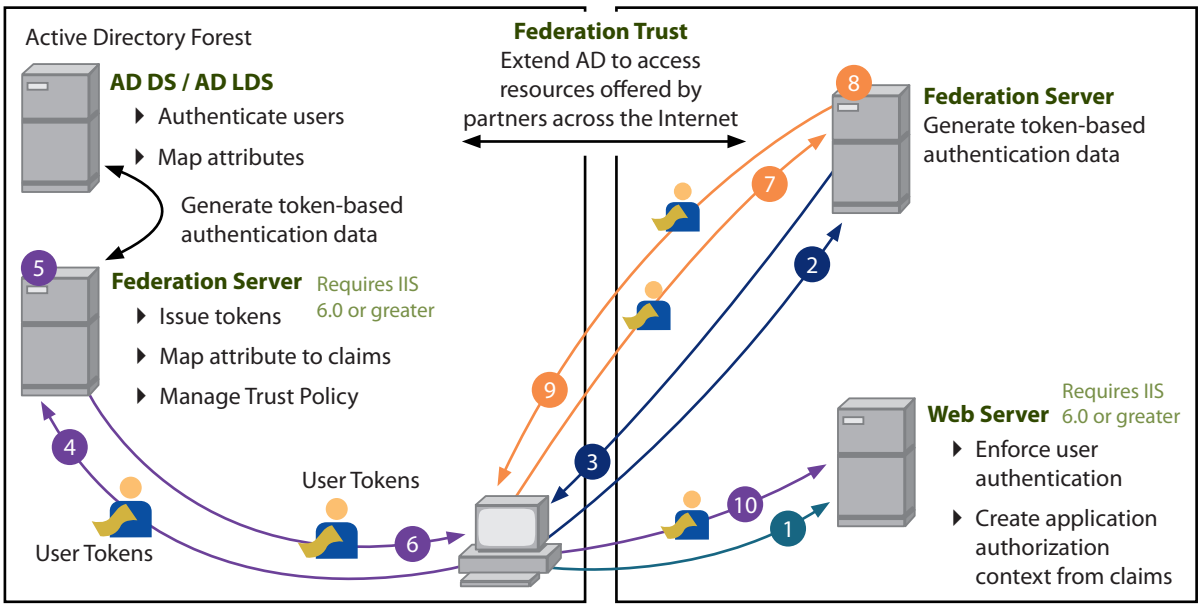
Federation Scenarios

Federated Web SSO with Forest Trust
Forests located in the DMZ and internal network. A federation trust is established so accounts in internal forest can access Web-based applications in perimeter network (including intranet or Internet access).

Web SSO
Users must authenticate only once to access multiple Web-based applications. All users are external, and no federation trust exists.

Federated Web SSO
Federation trust relationship established between two businesses. FS routes authentication requests from user accounts in "adatum" to Web-based applications that are located in the "treyresearch" network.

AD FS Authentication Flow



1. Client tries to access Web application in treyresearch.net. Web server requests token for access.
2. Client redirect to Federation Server on treyresearch.net. Federation server has list of partners that have access to the Web application. Refers client to its adatum.com Federation Server.
3. Instruct client to get a token from adatum.com Federation Server.
4. Client is member of its domain. Presents user authentication data to adatum.com Federation Server.
5. Based on authentication data, SAML token generated for the client.
6. User obtains SAML token from adatum.com Federation Server for treyresearch.net Federation Server.
7. Redirects client to treyresearch.net Federation Server for claims management.
8. Based on policies for the claims presented by the adatum.com token, a treyresearch.net token for the Web application is generated for the client.
9. The treyresearch.net token is delivered to client.
10. Client can now present treyresearch.net token to Web server to gain access to the application.

Active Directory Management

Fine-Grained Password Policies

Fine-grained password policy removes the restriction of a single password policy per domain.

Requires Windows Server 2008 Domain Mode

Set Attributes on PasswordSettings Object:

- Precedence
- Password Settings
- Account Lockout Settings
- Distinguished Name of Users and/or Groups the settings apply to

msDS-Password-SettingsObject(s)

Applied to Users and/or Groups

PasswordSettings objects stored in ...

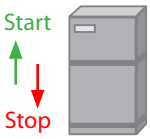
Password Settings Container

cn=Password Settings Container, cn=System, dc=northwind, dc=com

At User Logon and Password Change, check if a Password Settings Object has been assigned to this user

Restartable Active Directory Service

Active Directory Domain Services (AD DS) in Windows Server 2008 has the capability to start and stop the Active Directory Service via the MMC or command line



Restartable DS

Restarting AD requires membership of the built-in Administrators group on the DC

Stop/Start DS without Reboot

- If the DC is contacted while the DC service is stopped, server acts as member server
- Another DC is used for logon, and normal Group Policy is applied

If another DC cannot be contacted, administrator can log on either by using cached credentials or using the DSRM credentials

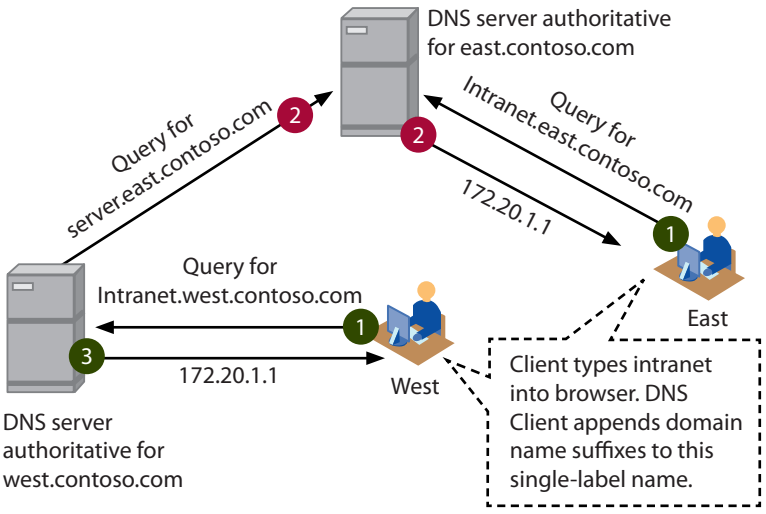
Directory Service States

- AD DS Started
- AD DS Stopped (Ntds.dit offline)
- AD Directory Restore Mode

GlobalNames Zone

Resolution of single-label, static, global names for servers using DNS.

- All authoritative DNS servers for a domain must be running Windows Server 2008 to provide GlobalNames support for clients
- Implemented as a Regular Forward Lookup zone, which must be named "GlobalNames"
- GlobalNames zone should be Active Directory integrated and replicated forest-wide
- The GlobalNames zone is manually configured with CNAME records to redirect from server's host name to Fully Qualified Domain Name



Domain Controller

DNS Information

The following types of Zones are now Available in Windows Server 2008 and can be used in accordance with your DNS design. Additionally, Microsoft frequently likes to test on the difference between these different types of Zones on MCTS and MCITP level exams. Table 1 should answer these questions effectively.

Zone Type	Description
Primary	A primary zone is the primary source for information about this zone, and it stores the master copy of zone data in a local file or in AD DS. When the zone is stored in a file, by default, the primary zone file is named *zone_name*.dns and is located in the %windir%\System32\Dns folder on the server.
Secondary	A secondary zone is the secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone. This DNS server must have network access to the remote DNS server that supplies it with updated information about the zone. Because a secondary zone is merely a copy of a primary zone that is hosted on another server, it cannot be stored in AD DS.
Stub	A stub zone is a copy of a zone that contains only the resource records that are necessary to identify the authoritative DNS servers for that zone. A stub zone keeps a DNS server hosting a parent zone aware of the authoritative DNS servers for its child zone. This helps maintain DNS name-resolution efficiency.
GlobalNames	The GlobalNames zone was added in Windows Server 2008 to hold single-label names and provide support for organizations still utilizing WINS. Unlike WINS, the GlobalNames zone is intended to provide single-label name resolution for a limited set of host names, typically corporate servers and Web sites that are centrally (IT) managed. The GlobalNames zone is not intended to be used for peer-to-peer name resolution, such as name resolution for workstations, and dynamic updates in the GlobalNames zone are not supported. Instead, the GlobalNames zone is most commonly used to hold CNAME resource records to map a single-label name to a fully qualified domain name (FQDN).
Forward lookup	Forward lookup zones support the primary function of Domain Name System (DNS), that is, the resolution of host names to IP addresses. Forward lookup zones provide name-to-address resolution.
Reverse lookup	A reverse lookup zone contains pointer (PTR) resource records that map IP addresses to the host name. Some applications, such as secure Web applications, rely on reverse lookups.

Windows Server 2008 Available Domain and Forest Functional Levels

Windows Server 2008 has changed the functional level at which Windows Server can function. Now, the minimum level is Windows Server 2000 and the maximum is Windows Server 2008. Mixed mode is no longer available. Table 2 outlines these changes:

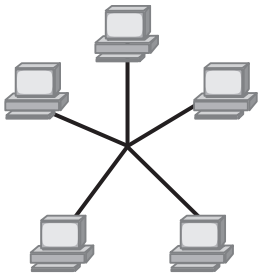
Domain Function Level	Available Features	SupportedDomain ControllerOperating Systems
Windows 2000 Native	All of the default AD DS features and the following directory features are available: ▸ Universal groups for distribution and security. ▸ Group nesting. ▸ Group conversion between security and distribution groups. ▸ Security identifier (SID) history.	Windows 2000 Windows Server 2003 Windows Server 2008
Windows Server 2003	All the default AD DS features, all the features that are available at the Windows 2000 native domain functional level, and the following features are available: ▸ *Netdom.exe* ▸ Logon time-stamp updates. ▸ Able to set the *userPassword* attribute as the effective password on *inetOrgPerson* and user objects. ▸ Able to redirect Users and Computers containers. ▸ Authorization Manager is able to store its authorization policies in AD DS. ▸ Constrained delegation. ▸ Selective authentication.	Windows Server 2003 Windows Server 2008
Windows Server 2008	All of the default AD DS features, all of thefeatures from the Windows Server 2003 domain functional level, and the following features are available: ▸ Distributed File System (DFS) replication support for the Windows Server 2003 SystemVolume (SYSVOL). ▸ Advanced Encryption Standard (AES 128 and AES 256) support Kerberos. ▸ Last Interactive Logon Information. ▸ Fine-grained password policies.	Windows Server 2008

Network Design

Part of the process of designing a functioning Windows Server 2008 network is to pick an appropriate design for your network. With Windows Server 2008 we are really limited to two appropriate logical topologies in order to maximize network bandwith. These two topologies are the Star and Mesh topology.

Star

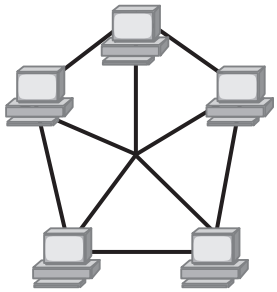
The Star topology is focused around a central network device, such as a switch or a router, and then extends out to external computers. With Windows Server 2008, this can even be a server running Windows Server 2008.



Star Topology

Mesh

A Mesh topology is a completed linked logical topology that is designed to provide redundancy in the case of the failure of one or two links connecting different computers. This is the preferred method for Windows Server 2008.

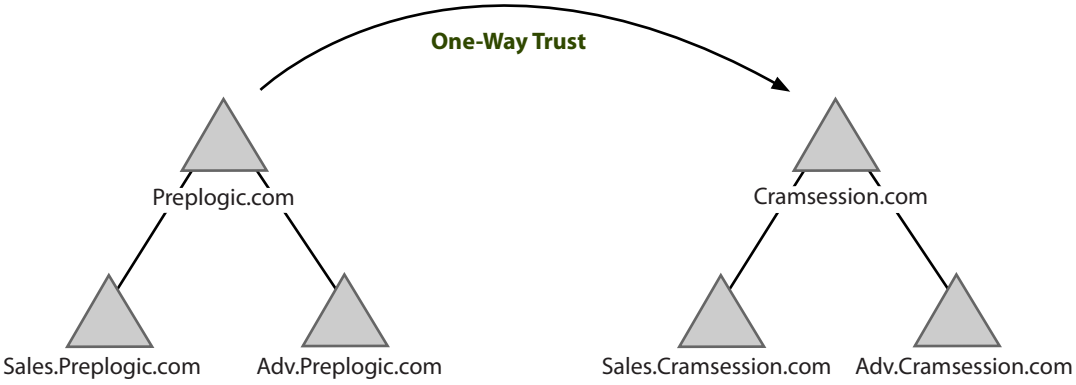


Mesh Topology

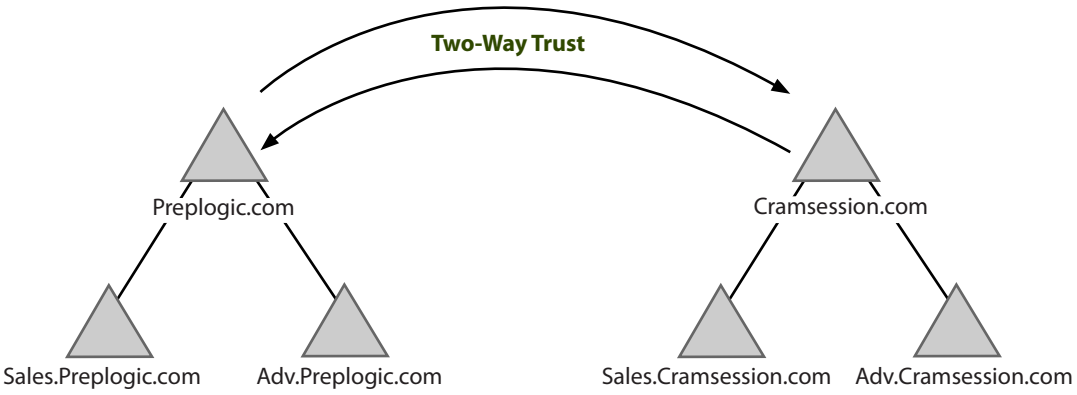
Forest Trusts

With Windows Server 2008 there are several different types of Domain and Forest trusts that we can choose from. In short, the following 5 diagrams here will summarize the different types available, as well as their advantages and disadvantages.

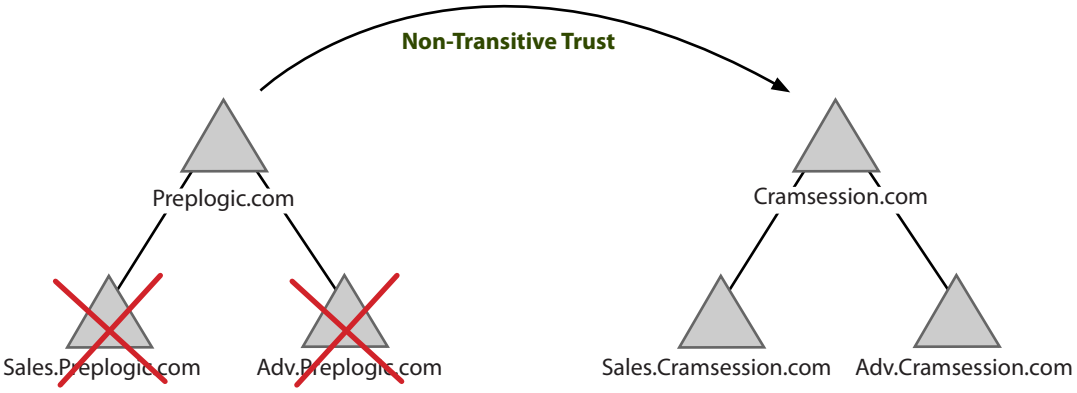
A one-way trust exists between either two forests or two domains and signifies a ONE-WAY trust between those forest or domains. In other words, the forest trust exists in a single direction. In the above example, LearnSmart.com would trust Cramsession.com because the forest trust points toward Cramsession. It's basically saying "I trust this!"



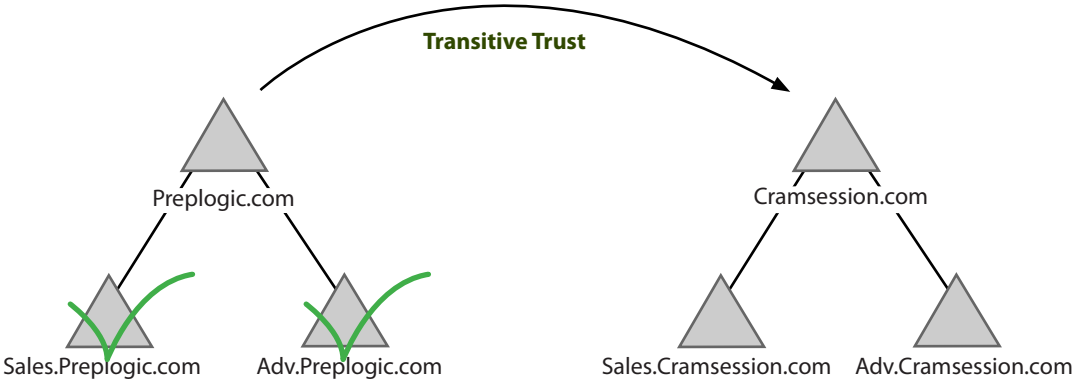
In a TWO-WAY trust, the trusts that exist between two forest or two domains exist in both directions. Technically, a two-way trust is effectively two one-way trusts. One forest says "I trust this" and the other forest says "I trust this."



Trusts in Windows Server 2008 farms (or earlier versions of Windows Server supporting Windows Active Directory) can exist in two forms: Transitive and Non-Transitive. With a non-transitive trust, the trust exists solely between two domains and doesn't necessarily extend to other domains. In the case above, PrepLogic.com trusts Cramsession.com, but the subdomains Sales.Preplogic.com and Adv.Preplogic.com do not trust Cramsession.com.

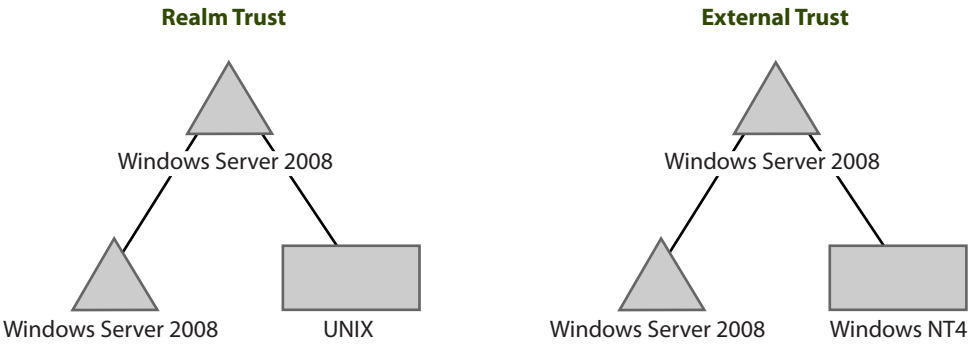


Using a Transitive Trust, Windows Server 2008 replicates this trust to all subdomains so that they trust each other as well as their parents. This method is used so domains do not have to be given explicit permission, but rather inherit it automatically.



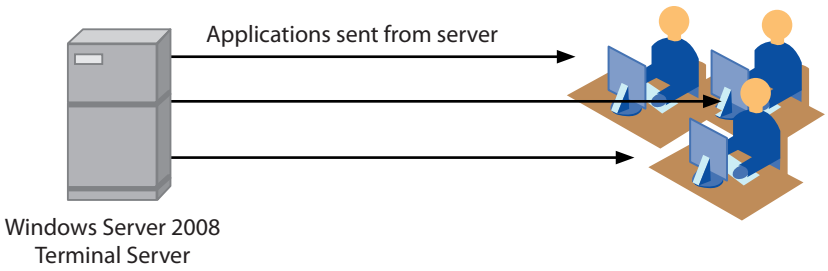
Additional Trust Types

Windows Server 2008 supports various trust types that can be used with infrastructures that do not support active directory. Namely, Windows Server 2008 supports External and Realm trusts. These two different types of trusts are used to support the UNIX and Windows NT4 (pre-active-directory) infrastructure. This allows an administrator to conveniently add in detail that isn't normally asssociated with Windows Active Directory with very little administrative effort.



Windows Server 2008 Terminal Services

Arguably Windows Server 2008's most powerful feature is its robust set of Terminal Services and Application Virtualization utilities, such as Remote Desktop, Application Virtualization, and Easy Print.

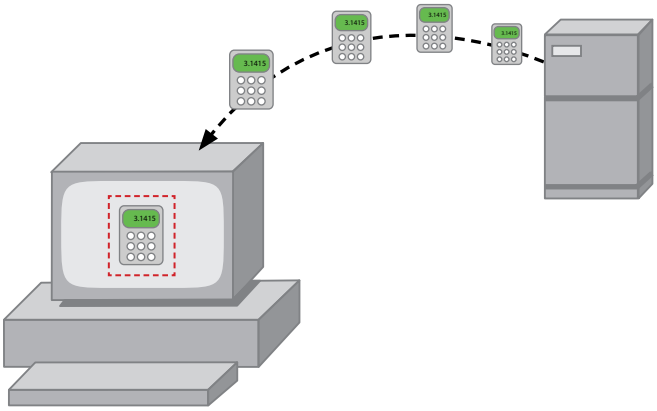


Remote Desktop

The simplest form of Terminal Services is Remote Desktop, which is an easy way of accessing a standard users's desktop over the TCP/IP protocol in a secure manner.

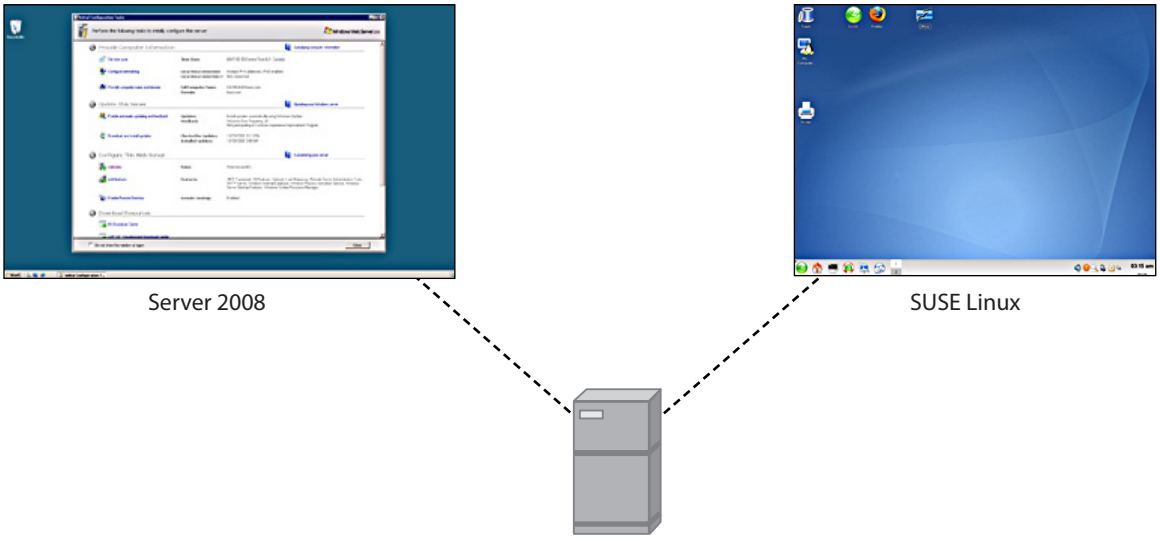
NOTE: Remote Desktop uses TCP/IP Port 3389.

Application Virtualization

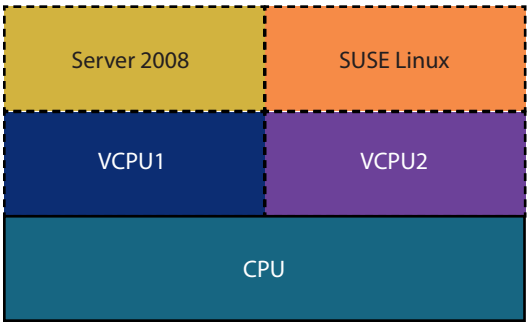


Application Virtualization is the concept of fooling a user into believing that an application is actually being run on their own local machine, but is actually being run on a remote server. In the above diagram, a calculator application is being run on our Windows Server 2008 server and then being accessed via terminal services by the client using Windows Vista.

The Windows Server 2008 Hypervisor



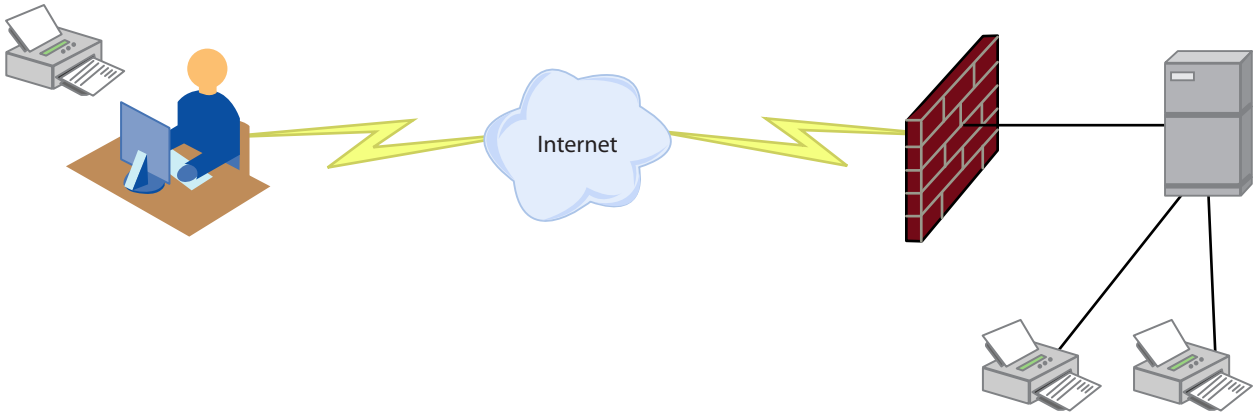
Using Windows Server 2008 Hyper-V, Windows Server 2008 can virtually emulate various operating systems produced both by Microsoft and other vendors at the hardware level through the use of virtualization technology that divides processors into logical units, as shown in the diagram below.



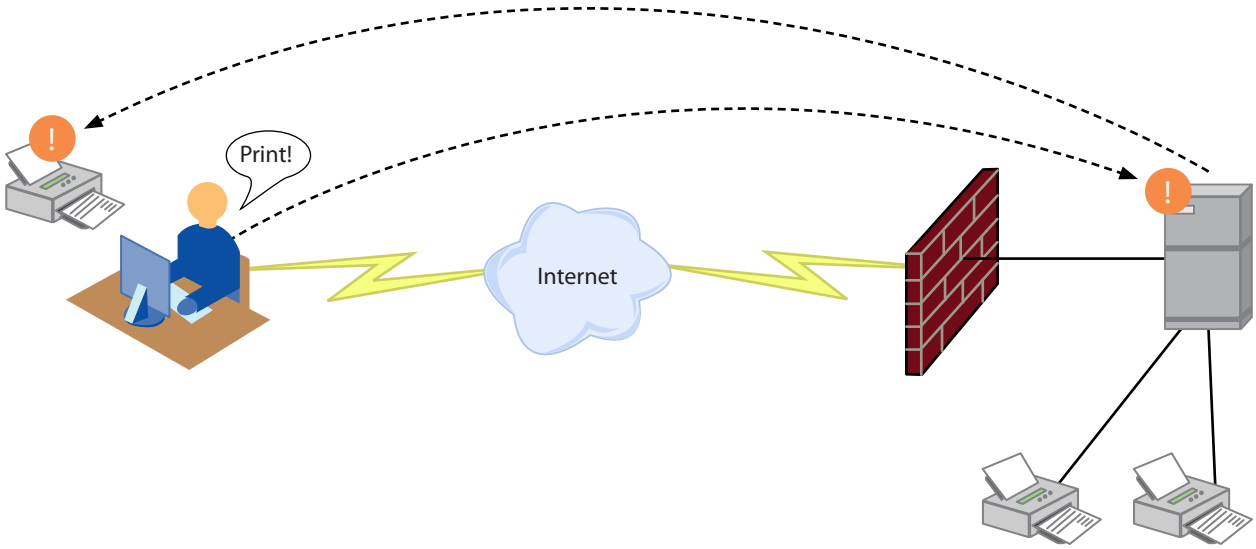
Using Hyper-V, Windows Server 2008 can divide a single CPU, or even multiple CPUs, into dedicated logical units. These virtual processors are divided between each other, running separate threads that stay completely apart. This way, multiple processors can have complete access to hardware components without interfering with the overall architecture of the platform.

Easy Print

One of the new features of Windows Server 2008 is "easy print." Before easy print, if a user was connected to an application through terminal services and pressed the "print" button, they may have accidentally caused the terminal server's printer to print, instead of their local printer. Now, instead of this occuring, easy print ensures that only the locally attached user printer will print.



In the diagram below, the user requests the server to print and the server tells the computer on the local user's network to print. To the user, it's as easy as simply pressing the "Print" button.



Preparing a Forest for Windows Server 2008

When you decided to use Windows Server 2008 in a current running environment, you're required to prepare the rest of your Windows Servers for the reception of a new Windows Server. The way this is achieved is by using a standard command, provided by Microsoft with official documentation. This command is adprep.

ADprep

Parameter	Description
/forestprep	This switch, combined with the Adprep command, prepares a forest for the introduction of a domain controller that runs Windows Server 2008. You run this command only once in the forest. You must run this command on the domain controller that holds the schema operations master role (also known as flexible single master operations or FSMO) for the forest. You must be a member of all the following groups to run this command: ▸ The Enterprise Admins group ▸ The Schema Admins group ▸ The Domain Admins group of the domain that hosts the schema master
/domainprep	Prepares a domain for the introduction of a domain controller that runs Windows Server 2008. You run this command after the forestprep command finishes and after the changes replicate to all the domain controllers in the forest. Run this command in each domain where you plan to add a domain controller that runs Windows Server 2008. You must run this command on the domain controller that holds the infrastructure operations master role for the domain. You must be a member of the Domain Admins group to run this command.
/domainprep /gpprep	Performs similar updates as domainprep. However, this command also provides updates that are necessary to enable Resultant Set of Policy (RSOP) Planning Mode functionality.
/rodcprep	Updates permissions on application directory partitions to enable replication of the partitions to read-only domain controllers (RODCs). This operation runs remotely; it contacts the infrastructure master in each domain to update the permissions. You need to run this command only once in the forest. However, you can rerun this command any time if it fails to complete successfully because an infrastructure master is not available. You can run this command on any computer in the forest. You must be a member of the Enterprise Admins group to run this command.
/wssg	Returns an expanded set of exit codes, instead of just 0 (Success) and 1 (Failure).
/silent	Specifies that no standard output is returned from an operation. This parameter can be used only if /wssg is also used.
quit	Returns to the prior menu.
Help	Displays Help for this command.
?	Displays Help for this command.

Configuring Active Directory Certificate Services

Obviously, one of the most important parts of Windows architecture is the Public Key Infrastructure. Using Windows Server 2008, we can use the Active Directory Certificate Services to setup our Server as a Certificate authority that can issue certificates to users, as well as several other important key functions. The manner in which this is done has chnaged since Windows Server 2008, but we've outlined it here in this section of the reference guide.

Install Active Directory Certificate Services

Follow the steps below to install an enterprise root CA:

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. In the **Roles Summary** section, click **Add roles**.
3. On the **Select Server Roles** page, select the **Active Directory Certificate Services** check box. Click **Next** two times.
4. On the **Select Role Services** page, select the **Certification Authority** check box, and click **Next**.
5. On the **Specify Setup Type** page, click **Enterprise**, and then click **Next**.
6. On the **Specify CA Type** page, click **Root CA**, and then click **Next**.
7. On the **Set Up Private Key** and **Configure Cryptography for CA** pages, you can configure optional configuration settings, including cryptographic service providers. Click **Next**.
8. In the **Common name for this CA** box, type the common name of the CA, and click **Next**.
9. On the **Set the Certificate Validity Period** page, accept the default validity duration for the root CA or specify a different duration, and click **Next**.
10. On the **Configure Certificate Database** page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and click **Next**.
11. After verifying the information on the **Confirm Installation Options** page, click **Install**.

Follow the steps below to install a stand-alone root CA:

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. In the **Roles Summary** section, click **Add roles**.
3. On the **Select Role Services** page, select the **Certification Authority** check box, and click **Next**.
4. On the **Specify Setup Type** page, click **Standalone**, and then click **Next**.
5. On the **Specify CA Type** page, click **Root CA**, and then click **Next**.
6. On the **Set Up Private Key** and **Configure Cryptography for CA** pages, you can configure optional settings, including cryptographic service providers. Click **Next**.
7. In the **Common name for this CA** box, type the common name of the CA, and click **Next**.
8. On the **Set the Certificate Validity Period** page, accept the default validity duration for the root CA, and click **Next**.
9. On the **Configure Certificate Database** page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and click **Next**.
10. After verifying the information on the **Confirm Installation Options** page, click **Install**.

Follow the steps below to set up a subordinate issuing CA:

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. In the **Roles Summary** section, click **Add roles**.
3. On the **Select Role Services** page, select the **Certification Authority** check box, and click **Next**.
4. On the **Specify Setup Type** page, click **Standalone** or **Enterprise**, and then click **Next**.
5. On the **Specify CA Type** page, click **Subordinate CA**, and then click **Next**.
6. On the **Set Up Private Key** and **Configure Cryptography for CA** pages, you can configure optional settings, including cryptographic service providers. Click **Next**.
7. On the **Request Certificate** page, browse to locate the root CA, or if the root CA is not connected to the network, save the certificate request to a file so that it can be processed later. Click **Next**.

- The subordinate CA setup will not be usable until it has been issued a root CA certificate and this certificate has been used to complete the installation of the subordinate CA.

8. In the **Common name for this CA** box, type the common name of the CA.
9. On the **Set the Certificate Validity Period** page, accept the default validity duration for the CA, and click **Next**.
10. On the **Configure Certificate Database** page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and click **Next**.
11. After verifying the information on the **Confirm Installation Options** page, click **Install**.

Configure CA server settings

The basic steps for configuring a CA for key archival are:

1. Create a key recovery agent account or designate an existing user to serve as the key recovery agent.
2. Configure the key recovery agent certificate template and enroll the key recovery agent for a key recovery agent certificate.
3. Register the new key recovery agent with the CA.
4. Configure a certificate template, such as Basic EFS, for key archival, and enroll users for the new certificate. If users already have EFS certificates, ensure that the new certificate will supersede the certificate that does not include key archival.
5. Enroll users for encryption certificates based on the new certificate template.

- Users are not protected by key archival until they have enrolled for a certificate that has key recovery enabled. If they have certificates that were issued before key recovery was enabled, data encrypted with these certificates will not be covered by key archival.

Follow the steps below to back up a CA by using the Certification Authority snap-in:

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, point to **All Tasks**, and click **Back Up CA**.
4. Follow the instructions in the CA Backup Wizard.

Follow the steps below to back up a CA by using the *Certutil* command-line tool:

1. Open a command prompt.
2. Type **certutil -backup <BackupDirectory>**, where *BackupDirectory* is the path used to store the backup data.
3. Press **Enter**.

Follow the steps below to restore a CA from a backup copy by using the Certification Authority snap-in:

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, point to **All Tasks**, and click **Restore CA**.
4. Follow the instructions in the Certification Authority Restore Wizard.

Follow the steps below to restore a CA by using the *Certutil* command-line tool:

1. Open a command prompt.
2. Type **certutil -restore <*BackupDirectory*>**, where *BackupDirectory* specifies the path where the backup data is located.
3. Press **Enter**.

Manage certificate templates

The following table lists and defines the different certificate templates available in Windows Server 2008:

Name	Description	Key Usage	Applications used for extended key usage (EKU)
Administrator	Allows trust list signing and user authentication	Signature and encryption	Microsoft Trust List Signing EFS Secure Email Client Authentication
Authenticated Session	Allows subject to authenticate to a Web server	Signature	Client Authentication
Basic EFS	Used by Encrypting File System (EFS) to encrypt data	Encryption	EFS
CA Exchange	Used to protect private keys as they are sent to the CA for private key archival	Encryption	Private Key Archival
CEP Encryption	Allows the holder to act as a registration authority (RA) for simple certificate enrollment protocol (SCEP) requests. (The Windows Server 2008 NDES uses this template, by default, for its key exchange certificate to keep communications with devices secret.)	Encryption	Certificate Request Agent
Code Signing	Used to digitally sign software	Signature	Code Signing
Computer	Allows a computer to authenticate itself on the network	Signature and encryption	Client Authentication Server Authentication
Cross-Certification Authority	Used for cross-certification and qualified subordination.	Signature Certificate signing CRL signing	
Directory E-mail Replication	Used to replicate e-mail within Active Directory	Signature and encryption	Directory Service E-mail Replication
Domain Controller	All-purpose certificates used by domain controllers (Superseded by two separate templates: Domain Controller Authentication and Directory E-mail replication)	Signature and encryption	Client Authentication Server Authentication
Domain Controller Authentication	Used to authenticate Active Directory computers and users	Signature and encryption	Client Authentication Server Authentication Smart Card Logon
EFS Recovery Agent	Allows the subject to decrypt files previously encrypted with EFS	Encryption	File Recovery
Enrollment Agent	Used to request certificates on behalf of another subject	Signature	Certificate Request Agent
Enrollment Agent (Computer)	Used to request certificates on behalf of another computer subject	Signature	Certificate Request Agent

Table continued on next page

Exchange Enrollment Agent (Offline request)	Used to request certificates on behalf of another subject and supply the subject name in the request (The Windows Server 2008 NDES uses this template for its enrollment agent certificate, by default.)	Signature	Certificate Request Agent
Exchange Signature Only	Used by Microsoft Exchange Key Management Service to issue certificates to Exchange users for digitally signing e-mail	Signature	Secure E-mail
Exchange User	Used by Exchange Key Management Service to issue certificates to Exchange users for encrypting e-mail	Encryption	Secure E-mail
IPSec	Used by IPSec to digitally sign, encrypt, and decrypt network communication	Signature and encryption	IPSec Internet Key Exchange (IKE) intermediate
IPSec (Offline request)	Used by IPSec to digitally sign, encrypt, and decrypt network communication when the subject name is supplied in the request. (The Windows Server 2008 SCEP service uses this template, by default, for device certificates.)	Signature and encryption	IPSec IKE intermediate
Kerberos Authentication	New in Windows Server 2008, this template is similar to the "Domain Controller Authentication" template and offers enhanced security capabilities for Windows Server 2008 domain controllers authenticating Active Directory users and computers.	Signature and Encryption	Client Authentication Server Authentication Smart Card Logon KDC Authentication
Key Recovery Agent (KRA)	Recovers private keys that are archived on the CA.	Encryption	Key Recovery Agent
OCSP Response Signing	New in Windows Server 2008, this template issues certificates used by the OCSP Service Provider to sign OCSP responses. (By default, these certificates contain a special "OCSP No Revocation Checking" extension and no AIA or CDP extensions.)	Signature	OCSP Signing
Remote Access Service (RAS) and Internet Authentication Service (IAS) Server	Enables RAS and IAS servers to authenticate their identity to other computers	Signature and Encryption	Client Authentication Server Authentication
Root CA	Used to prove the identity of the root CA	Signature Certificate signing CRL signing	
Router (Offline request)	Used by a router when requested through SCEP from a CA that holds a CEP Encryption certificate	Signature and encryption	Client Authentication

Table continued on next page

Smart Card Logon	Allows the holder to authenticate using a smart card	Signature and encryption	Client Authentication Smart Card Logon
Smart Card User	Allows the holder to authenticate and protect e-mail using a smart card	Signature and encryption	Secure E-mail Client Authentication Smart Card Logon
Subordinate CA	Used to prove the identity of the subordinate CA. It is issued by the parent or root CA.	Signature Certificate signing CRL signing	
Trust List Signing	Allows the holder to digitally sign a trust list	Signature	Microsoft Trust List Signing
User	Used by users for e-mail, EFS, and client authentication	Signature and encryption	EFS Secure E-mail Key Usage
User Signature Only	Allows users to digitally sign data	Signature	Secure E-mail Client Authentication
Web Server	Proves the identity of a Web server	Signature and encryption	Server Authentication
Workstation Authentication	Enables client computers to authenticate their identity to servers	Signature and encryption	Client Authentication

Follow the steps below to add a certificate template to a CA:

1. Open the Certification Authority snap-in, and double-click the name of the CA.
2. Right-click the Certificate Templates container; click **New**, and then click **Certificate Template to Issue**.
3. Select the certificate template, and click **OK**.

Follow the steps below to set CA administrator and certificate manager security permissions for a CA:

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, click **Properties**.
4. Click the **Security** tab, and specify the security permissions.

Follow the steps below to define permissions to allow a specific security principal to enroll for certificates based on a certificate template:

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the **Certificate Templates** MMC (*Certtmpl.msc*).
3. In the details pane, right-click the certificate template you want to change, and then click **Properties**.
4. On the **Security** tab, ensure that **Authenticated users** is assigned **Read** permissions.
    - This ensures that all authenticated users on the network can see the certificate templates.
5. On the **Security** tab, click **Add**. Add a global group or universal group that contains all security principals requiring Enroll permissions for the certificate template, and click **OK**.
6. On the **Security** tab, select the newly added security group, and then assign **Allow** permissions for the **Read and Enroll** permissions.
7. Click **OK**.

Follow the steps below to configure a key recovery agent:

1. Log on as Administrator of the server or CA Administrator, if role separation is enabled.
2. On the **Administrative Tools** menu, open **Certification Authority**.
3. In the console tree, select the CA.
4. Right-click the CA name, and then click **Properties**.
5. Click the **Recovery Agents** tab.
6. To enable key archival, click **Archive the key**.
7. By default, the CA will only use one KRA. However, a KRA certificate must first be selected for the CA to begin archival. To select a KRA certificate, click **Add**.

   The system will find valid KRA certificates and display the available KRA certificates. KRA certificates are normally published to Active Directory by an Enterprise CA when enrollment occurs. KRA certificates are stored under the KRA container in the Public Key Services branch of the configuration partition in Active Directory. Since a CA may issue multiple KRA certificates, each KRA certificate will be added to the multi-valued userAttribute attribute of the CA object.
8. Select one certificate and click **OK**. You may view the highlighted certificate to ensure that you have selected the intended certificate.
9. After one or more KRA certificates have been added, click **OK** to enable key archival on the CA. However, Certificate Services must be stopped and started to enable the use of the selected KRAs. KRA certificates are only processed at service start.

Manage enrollments

Follow the steps below to configure the default action for certificate requests:

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, click **Properties**.
4. On the **Policy Module** tab, click **Properties**.
5. Click the option you want:
   a. To have the CA administrator review every certificate request before issuing a certificate, click **Set the certificate request status to pending**.
   b. To have the CA issue certificates based on the configuration of the certificate template, click **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**.
6. Stop and restart the CA.

Follow the steps below to set up and configure the Network Device Enrollment Service (NDES):

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. In the **Roles Summary** section, click **Add roles**.
3. On the **Select Role Services** page, clear the **Certification Authority** check box, and select **Network Device Enrollment Service**.
   - Unless already installed on the selected server, you are prompted to install IIS and Windows Activation Service.
4. Click **Add Required Role Services**, and then click **Next** three times.
5. On the **Confirm Installation Options** page, click **Install**.
6. When the installation is complete, review the status page to verify that the installation was successful.
7. If this is a new installation with no pending SCEP certificate requests, click **Replace existing Registration Authority (RA) certificates**, and then click **Next**.
   - **NOTE**: When the Network Device Enrollment Service is installed on a computer where a registration authority already exists, the existing registration authority, and any pending certificate requests, are deleted.

8. On the **Specify User Account** page, click **Select User**, and type the user name and password for this account, which the Network Device Enrollment Service will use to authorize certificate requests. Click **OK**, and then click **Next**.
9. On the **Specify CA** page, select either the **CA name** or **Computer name** check box; click **Browse** to locate the CA that will issue the Network Device Enrollment Service certificates, and then click **Next**.
10. On the **Specify Registry Authority Information** page, type computer name in the **RA name** box. Under **Country/region**, select the check box for the country/region you are in, and click **Next**.
11. On the **Configure Cryptography** page, accept the default values for the signature and encryption keys, and click **Next**.
12. Review the summary of configuration options, and click **Install**.

Follow the steps below to configure the autoenrollment options in Group Policy:

1. On a domain controller running Windows Server 2008, click **Start**; point to **Administrative Tools**, and click **Group Policy Management**.
2. In the console tree, double-click **Group Policy Objects** in the forest and domain containing the **Default Domain Policy** Group Policy object (GPO) that you want to edit.
3. Right-click the **Default Domain Policy** GPO, and then click **Edit**.
4. In the Group Policy Management Console (GPMC), go to **User Configuration**, **Windows Settings**, **Security Settings**, and click **Public Key Policies**.
5. Double-click **Certificate Services Client - Auto-Enrollment**.
6. Select the **Enroll certificates automatically** check box to enable autoenrollment. If you want to block autoenrollment from occurring, select the **Do not enroll certificates automatically** check box.
7. If you are enabling certificate autoenrollment, you can select the following check boxes:
    a. Renew expired certificates, update pending certificates, and remove revoked certificates
    b. Update certificates that use certificate templates
8. Click **OK** to accept your changes.

Follow the steps below to install Web enrollment support:

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. Click **Manage Roles**. Under **Active Directory Certificate Services**, click **Add role services**. If a different AD CS role service has already been installed on this computer, select the **Active Directory Certificate Services** check box in the **Role Summary** pane, and click **Add role services**.
3. On the **Select Role Services** page, select the **Certification AuthorityWeb Enrollment Support** check box.
4. Click **Add required role services**, and then click **Next**.
5. On the **Specify CA** page, if a CA is not installed on this computer, click **Browse** to select the CA that you want to associate with Web enrollment; click **OK**, and then **Next**.
6. Click **Next**; review the information listed, and click **Next** again.
7. On the **Confirm Installation Options** page, click **Install**.
8. When the installation is complete, review the status page to verify that the installation was successful.

Follow the steps below to configure an Enterprise CA to issue a KRA certificate for use with smart card enrollment:

1. On the **Administrative Tools** menu, open the **Certification Authority** snap-in.
2. In the console tree, expand **Certification Authority**, and click **Certificate Templates**.
3. Right-click the **Certificate Templates** node; click **New**, and then click **Certificate Template to Issue**.
4. In the **Select Certificate Template** dialog box, click **Key Recovery Agent**, and then click **OK.**
5. Close the **Certification Authority** MMC snap-in.

Follow the steps below to define permissions to allow a specific security principal to enroll for certificates based on a certificate template

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the **Certificate Templates** MMC (Certtmpl.msc).
3. In the details pane, right-click the certificate template you want to change, and then click **Properties**.
4. On the **Security** tab, ensure that **Authenticated users** is assigned **Read** permissions.
    - This ensures that all authenticated users on the network can see the certificate templates.
5. On the **Security** tab, click **Add**. Add a global group or universal group that contains all security principals requiring Enroll permissions for the certificate template, and click **OK**.
6. On the **Security** tab, select the newly added security group, and then assign **Allow** permissions for the **Read and Enroll** permissions.
7. Click **OK**.

Manage certificate revocations

Follow the steps below to install the Online Responder:

1. Ensure that IIS has already been installed on the Windows Server 2008 computer.
2. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
3. Click **Manage Roles**. In the **Active Directory Certificate Services** section, click **Add role services**.
4. On the **Select Role Services** page, select the **Online Responder** check box.
5. You are prompted to install IIS and Windows Activation Service.
6. Click **Add Required Role Services**, and then click **Next** three times.
7. On the **Confirm Installation Options** page, click **Install**.

Follow the steps below to configure the CA for OCSP Response Signing certificates:

1. Log on to the server as a CA administrator.
2. Open the Certificate Templates snap-in.
3. Right-click the **OCSP Response Signing** template, and then click **Duplicate Template**.
4. Type a new name for the duplicated template.
5. Right-click the new certificate template, and then click **Properties**.
6. Click the **Security** tab. Under **Group or user name**, click **Add**, and type the name or browse to select the computer that will be hosting the Online Responder service.
7. Click the computer name, and in the **Permissions** dialog box, select the **Read** and **Autoenroll** check boxes.
8. While you have the Certificate Templates snap-in open, you can configure certificate templates for users and computers by substituting the desired templates in step 3, and repeating steps 4 through 7 to configure additional permissions for the server and your user accounts.

Follow the steps below to configure a CA to support the Online Responder service:

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, click **Properties**.
4. Click the **Extensions** tab. In the Select extension list, click **Authority Information Access (AIA)**.
5. Select the **Include in the AIA extension of issue certificates** and **Include in the online certificate status protocol (OCSP)** extension check boxes.
6. Specify the locations from which users can obtain certificate revocation data.
7. In the console tree of the Certification Authority snap-in, right-click **Certificate Templates**, and then click **New Certificate Templates to Issue**.

8. In **Enable Certificate Templates**, select the **OCSP Response Signing** template and any other certificate templates that you configured previously, and click **OK**.
9. Open **Certificate Templates**, and verify that the modified certificate templates appear in the list.

Follow the steps below to create a revocation configuration:

1. Open the Online Responder snap-in.
2. In the **Actions** pane, click **Add Revocation Configuration** to start the Add Revocation Configuration wizard, and then click **Next**.
3. On the **Name the Revocation Configuration** page, type a name for the revocation configuration, and click **Next**.
4. On the **Select CA certificate Location** page, click **Select a certificate from an existing enterprise CA**, and then click **Next**.
5. On the following page, the name of the CA should appear in the **Browse CA certificates published in Active Directory** box.
    a. If it appears, click the name of the CA that you want to associate with your revocation configuration, and then click **Next**.
    b. If it does not appear, click **Browse for a CA by Computer name** and type the name of the computer, or click **Browse** to locate this computer. When you have located the computer, click **Next**.
    c. You might also be able to link to the CA certificate from the local certificate store or by importing it from removable media in step 4.
6. View the certificate and copy the CRL distribution point for the parent root CA. To do this:
    1. Open the Certificate Services snap-in. Select an issued certificate.
    2. Double-click the certificate, and then click the **Details** tab.
    3. Scroll down and select the **CRL Distribution Points** field.
    4. Select and copy the URL for the CRL distribution point that you want to use.
    5. Click **OK**.
7. On the Select Signing Certificate page, accept the default option, **Automatically select signing certificate**, and click Next.
8. On the Revocation Provider page, click **Provider**.
9. On the **Revocation Provider Properties** page, click **Add**; enter the URL of the CRL distribution point, and click **OK**.
10. Click **Finish**.
11. Using the Online Responder snap-in, select the revocation configuration, and then examine the status information to verify that it is functioning properly. You should also be able to examine the properties of the signing certificate to verify that the Online Responder is configured properly.

Follow the steps below to revoke a certificate:

1. Open the Certification Authority snap-in.
2. In the console tree, click **Issued Certificates**.
3. In the details pane, click the certificate you want to revoke.
4. On the **Action** menu, point to **All Tasks**, and click **Revoke Certificate**.
5. Select the reason for revoking the certificate; adjust the time of the revocation, if necessary, and then click **Yes**. Available reason codes are:
    a. Unspecified
    b. Key Compromise
    c. CA Compromise
    d. Change of Affiliation
    e. Superseded
    f. Cease of Operation
    g. Certificate Hold. This is the only reason code that can be used when you might want to unrevoke the certificate in the future.

Follow the steps below to configure the Authority Information Access (AIA) extension:

1. Open the Certification Authority snap-in; right-click the name of the issuing CA, and then click **Properties**.
2. Click the **Extensions** tab.
3. In the **Select extension** list, click **Authority Information Access (AIA)**, and then click **Add**.
4. In the **Add Location** dialog box, type the full URL of the Online Responder, which should be in the following form: http://*<DNSServerName>*/*<vDir>*
    - **NOTE**: When installing the Online Responder, the default virtual directory used in IIS is OCSP.
5. Click **OK**.
6. Select the location from the **Location** list.
7. Select the **Include in the online certificate status protocol (OCSP) extension** check box, and click **OK**.

RepAdmin

Parameter	Description
Repadmin /kcc	Forces the Knowledge Consistency Checker (KCC) on targeted domain controllers to immediately recalculate the inbound replication topology.
Repadmin /prp	Specifies the Password Replication Policy (PRP) for read-only domain controllers (RODCs).
Repadmin /queue	Displays inbound replication requests that the domain controller must issue to become consistent with its source replication partners.
Repadmin /replicate	Triggers the immediate replication of the specified directory partition to a destination domain controller from a source domain controller.
Repadmin /replsingleobj	Replicates a single object between any two domain controllers that have common directory partitions.
Repadmin /replsummary	Identifies domain controllers that are failing inbound replication or outbound replication, and summarizes the results in a report.
Repadmin /rodcpwdrepl	Triggers replication of passwords for the specified users from the source domain controller to one or more read-only domain controllers. (The source domain controller is typically a hub site domain controller.)
Repadmin /showattr	Displays the attributes of an object.
Repadmin /showobjmeta	Displays the replication metadata for a specified object that is stored in AD DS, such as attribute ID, version number, originating and local update sequence numbers (USNs), globally unique identifier (GUID) of the originating server, and date and time stamp.
Repadmin /showrepl	Displays the replication status when the specified domain controller last attempted to perform inbound replication on Active Directory partitions.
Repadmin /showutdvec	Displays the highest, committed USN that AD DS, on the targeted domain controller, shows as committed for itself and its transitive partners.
Repadmin /syncall	Synchronizes a specified domain controller with all replication partners.

MountVol

Parameter	Description
[<Drive>:]<Path>	Specifies the existing NTFS directory where the mount point will reside.
<VolumeName>	Specifies the volume name that is the target of the mount point. The volume name uses the following syntax, where GUID is a globally unique identifier: ▸ \\?\Volume\{GUID}\ The brackets { } are required.
/d	Removes the volume mount point from the specified folder.
/l	Lists the mounted volume name for the specified folder.
/p	Removes the volume mount point from the specified directory, dismounts the basic volume, and takes the basic volume offline, making it unmountable. If other processes are using the volume, mountvol closes any open handles before dismounting the volume.
/r	Removes volume mount point directories and registry settings for volumes that are no longer in the system, preventing them from being automatically mounted and given their former volume mount point(s) when added back to the system.
/n	Disables automatic mounting of new basic volumes. New volumes are not mounted automatically when added to the system.
/e	Re-enables automatic mounting of new basic volumes.
/s	Mounts the EFI system partition on the specified drive. Available on Itanium-based computers only.
/?	Displays help at the command prompt.

Mount

Term	Definition
-o rsize=<buffersize>	Sets the size in kilobytes of the read buffer. Acceptable values are 1, 2, 4, 8, 16, and 32; the default is 32 KB.
-o wsize=<buffersize>	Sets the size in kilobytes of the write buffer. Acceptable values are 1, 2, 4, 8, 16, and 32; the default is 32 KB.
-o timeout=<seconds>	Sets the time-out value in seconds for a remote procedure call (RPC). Acceptable values are 0.8, 0.9, and any integer in the range 1-60; the default is 0.8.
-o retry=<number>	Sets the number of retries for a soft mount. Acceptable values are integers in the range 1-10; the default is 1.
-o mtype={soft | hard}	Sets the mount type (default is soft). Regardless of the mount type, mount will return if it cannot immediately mount the share. Once the share has been successfully mounted, however, if the mount type is hard, Client for NFS will continue to try to access the share until it is successful. As a result, if the NFS server is unavailable, any Windows program trying to access the share will appear to stop responding, or "hang," if the mount type is hard.
-o anon	Mounts as an anonymous user.

Table continued on next page

-o nolock	Disables locking (default is enabled).
-o casesensitive	Forces file lookups on the server to be case sensitive.
-o fileaccess=<mode>	Specifies the default permission mode of new files created on the NFS share. Specify mode as a three-digit number in the form ogw, where o, g, and w are each a digit representing the access granted the file's owner, group, and the world, respectively. The digits must be in the range 0-7 with the following meaning: ▸ 0: No access ▸ 1: x (execute access) ▸ 2: w (write access) ▸ 3: wx ▸ 4: r (read access) ▸ 5: rx ▸ 6: rw ▸ 7: rwx
-o lang={euc-jp|euc-tw|euc-kr|shift-jis|big5|ksc5601|gb2312-80|ansi}	Specifies the default encoding used for file and directory names and, if used, must be set to one of the following: ▸ ansi ▸ big5 (Chinese) ▸ euc-jp (Japanese) ▸ euc-kr (Korean) ▸ euc-tw (Chinese) ▸ gb2312-80 (Simplified Chinese) ▸ ksc5601 (Korean) ▸ shift-jis (Japanese) If this option is set to ansi on systems configured for non-English locales, the encoding scheme is set to the default encoding scheme for the locale. The following are the default encoding schemes for the indicated locales: ▸ Japanese: SHIFT-JIS ▸ Korean: KS_C_5601-1987 ▸ Simplified Chinese: GB2312-80 ▸ Traditional Chinese: BIG5
-u:<UserName>	Specifies the user name to use for mounting the share. If username is not preceded by a backslash (\), it is treated as a UNIX user name.
-p:<Password>	The password to use for mounting the share. If you use an asterisk (*), you will be prompted for the password.

DSmod

Command	Description
Dsmod computer	Modifies attributes of one or more existing computers in the directory.
Dsmod contact	Modifies attributes of one or more existing contacts in the directory.
Dsmod group	Modifies attributes of one or more existing groups in the directory.
Dsmod ou	Modifies attributes of one or more existing organizational units (OUs) in the directory.
Dsmod server	Modifies properties of a domain controller.
Dsmod user	Modifies attributes of one or more existing users in the directory.
Dsmod quota	Modifies attributes of one or more existing quota specifications in the directory.
Dsmod partition	Modifies attributes of one or more existing partitions in the directory.

DCPromo

Parameter	Description
/answer[:<filename>]	Specifies an answer file that contains installation parameters and values.
/unattend[:<filename>]	Specifies an answer file that contains installation parameters and values. This command provides the same function as /answer[:<filename>].
/unattend	Specifies an unattended installation in which you provide installation parameters and values at the command line.
/adv	Performs an install from media (IFM) operation.
/UninstallBinaries	Uninstalls AD DS binaries.
/CreateDCAccount	Creates a read-only domain controller (RODC) account. Only a member of the Domain Admins group or the Enterprise Admins group can run this command.
/UseExistingAccount:Attach	Attaches a server to an existing RODC account. A member of the Domain Admins group or a delegated user can run this command.
/?	Displays Help for Dcpromo parameters.
/?[:{Promotion | CreateDCAccount | UseExistingAccount | Demotion}]	Displays parameters that apply to the dcpromo operation. For example, dcpromo /?:Promotion displays all of the parameters that you can use for a promotion operation.

More Training for Windows Server 2008

We hope you've enjoyed your Windows Server 2008 Quick Reference Guide. But the Quick Reference Guide is only the beginning of your Server 2008 training. Microsoft has launched a full complement of certifications for Windows Server 2008. To find out how you can add these certifications to your transcript, contact the Microsoft Career Counselors at LearnSmart. They can help you navigate through the required exams and get the training you need to earn you Windows Server 2008 certifications. To learn more about training for Windows Server 2008, call LearnSmart at 1-800-418-6789.